

REMARKS

Claims 1-10 are pending in the present application. By virtue of this response, no claim has been cancelled or amended, and no new claim has been added. Accordingly, claims 1-10 are currently under consideration.

Claim Objections

Claims 7 and 8 were objected to because of the following informalities: “ROM” must be spelled out. In response, claims 7 and 8 have been amended to spell out “ROM” as Read Only Memory.

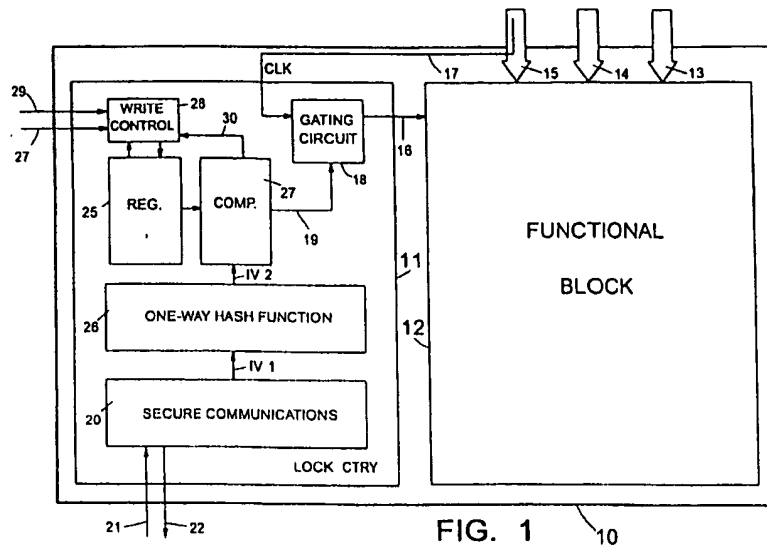
Rejections under 35 USC § 102

Claims 1-10 stand rejected under 35 USC § 102(b) as allegedly being anticipated by Vicard (US 5,708,715). Applicant respectfully traverses these rejections.

Applicant submits that the Vicard reference fails to disclose each and every element recited in independent claim 1. In particular, the Vicard reference fails to disclose at least the claim element of “a key means comprising a security release key.” Instead of providing such a key means in a lock circuitry, the cited reference requires a “chip-key” as an external input to the chip to unlock the lock circuitry. (See Vicard, column 4, lines 43-45.)

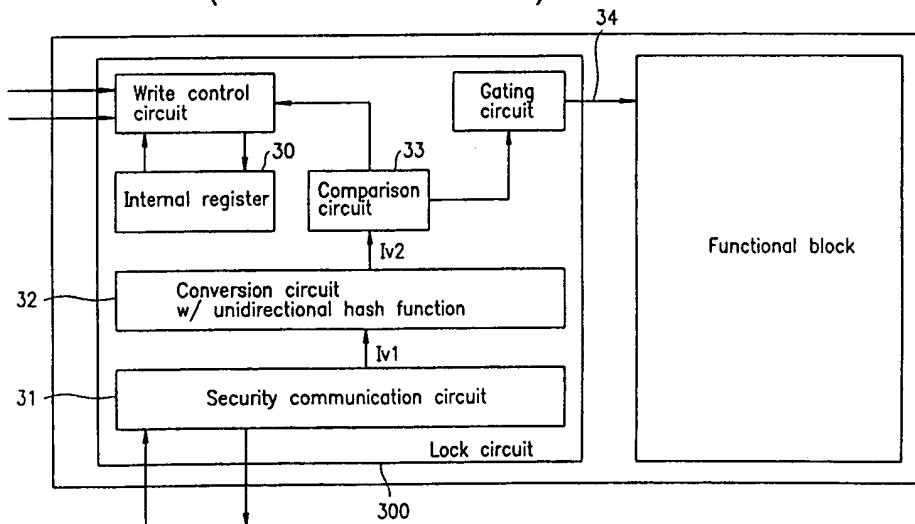
Applicant has disclosed the Vicard reference to the Office in the Information Disclosure Statement filed on June 28, 2001 that disclosed the European patent number EP0743602 and its U.S. equivalent US 5,708,715. Figure 1 of the Vicard reference and Figure 3 of the present application are shown below to illustrate that the Applicant has already distinguished the Vicard reference from the present invention in the Description of the Related Art section. (See page 2, line 14 to page 5, line 11.) The following discussion highlights the distinction between the Vicard reference and the present application, and supports the Applicant’s contention that the Vicard reference does not disclose at least the claim element of “a key means comprising a security release key.”

Comparison of FIG. 1 of the Vicard reference and FIG. 3 of the present application



U.S. Patent Jan. 13, 1998 Sheet 1 of 3 S,708,715

FIG. 3 (Conventional Art)



The present invention relates to a semiconductor storage device having a security function for preventing unauthorized tampering with any content stored in a memory. As stated in the section titled "Description of the related art", a semiconductor memory incorporating a conventional data tamper prevention circuit has a number of problems that are specifically addressed and mitigated by the present invention. Such a conventional circuit is shown in FIG. 1 of the cited reference and the conventional art diagram in FIG. 3 of the present application respectively. (See Figures above.) Note that both have identical block components within their respective lock circuitries and have identical principle of operation. Therefore, the cited reference has already been distinguished by the present invention, and it has the same problems that are addressed and mitigated by the present invention.

Specifically, the Abstract of the cited reference describes the operation of its lock circuitry as follows:

To unlock the lock circuitry, a "chip-key" must be supplied to the chip over a secure communications link, the chip-key being communicated in encrypted form and then decrypted in a secure communication block of the chip. To prevent internal examination of the chip revealing the chip key, the latter is not stored as such in the chip. Instead, only a signature of the chip-key is stored, the latter being formed from the chip-key by subjecting the latter to a one-way function. The chip-key input to the lock circuitry is subjected to the same one-way function in block before being compared with the stored chip-key in comparator; if a match is found, a gating circuit is enabled to pass a necessary signal (such as a clock signal) to the functional block. (Emphasis added; see also column 4, lines 20-67 and FIG. 1 of the cited reference)

The lock circuitry described above have a number of disadvantages. First, since the "chip-key" is retained external to the device, the chip-key must pass through an interfacing section, and as a result, it may be intercepted during communication or read directly from the external key storage device. (See page 4, lines 7-21.) Second, complicated circuitry is required for encrypting and decrypting inter-device signals. (See page 4, line 23 to page 5, line 4.) Third, in

order to incorporate such a conventional data tamper prevention circuit into a semiconductor storage device, the entire system must be redesigned to enable a good tamper prevention function. (See page 5, lines 6-11.)

To address the above problems of the conventional art, the present invention eliminates the need of an external chip-key input by storing a security release key in a memory region 12 of a non-volatile memory cell array block, along with the data to be protected. (See page 22, lines 3-9.) Meanwhile, the security registration lock is stored in a separate non-volatile register 13. (See page 22, lines 11-16.) In order to access the protected data, the security release key and the security registration lock have to “match”, where the match is determined by the determination circuit 14. The determination circuit may be implemented by subjecting the key and the lock to a predetermined mathematical operation, such as a unidirectional hash conversion. (See page 22, lines 20-25.) Therefore, even if either the key or the lock is illegally obtained or tampered by an unauthorized user, the data is still protected as both the key and the lock are required to access the data. In addition, since mathematical operations are used to “match” the key and the lock in the determination circuit, it is very hard to reverse-engineer the operations necessary to achieve a matching key and lock pair. The Vicard reference neither teaches nor suggests storing a security release key in a memory region of a non-volatile memory cell array. In addition, the Vicard reference does not disclose the matching of the security release key and the security registration lock described above. Instead, it requires an external “chip-key” input. Therefore, applicant asserts that the Vicard reference does not disclose a key means comprising a security release key recited in claim 1 of the present invention.

For the reasons presented above, the rejection of claim 1 should be withdrawn. In addition, the rejections of their corresponding dependent claims 2-10 should be withdrawn.

CONCLUSION

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of the claims and to pass this application to issue. If it is determined that a telephone conference would expedite the prosecution of this application, the Examiner is invited to telephone the undersigned at the number given below.

In the event the U.S. Patent and Trademark office determines that an extension and/or other relief is required, applicant petitions for any required relief including extensions of time and authorizes the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 03-1952 referencing docket no. **299002053200**. However, the Commissioner is not authorized to charge the cost of the issue fee to the Deposit Account.

Dated: August 4, 2006

Respectfully submitted,

By 

Thomas Chan

Registration No.: 51,543
MORRISON & FOERSTER LLP
755 Page Mill Road
Palo Alto, California 94304-1018
(650) 813-5616

AMENDMENTS TO THE DRAWINGS

The attached sheet of drawing includes changes to FIG. 3.

Attachment: Replacement sheet – FIG. 3